DPMM: dynamic pseudonym-based multiple mix-zones generation for mobile traveler

Imran Memon[1] · Qasim Ali[2] · Asma Zubedi[3] ·
Farman Ali Mangi[4]

Received: 21 February 2016 / Revised: 13 September 2016 / Accepted: 14 November 2016 /
Published online: 2 December 2016

Abstract Road traffic information has become indispensable for routine vehicular communication but user location privacy an important issue which did not well addressed. An adversary may attack a user by tracking location in routine vehicular communication. Although, continuously changing pseudonyms is a promising solution to attain location privacy in road networks, it has been observed that changing pseudonym at improper time or location may again become a threat for location preservation. As a result, a number of techniques for pseudonym-change have been proposed to achieve location privacy on road networks but most of location based services depend upon speed, GPS position and direction angle services. Hence, sensitive information is periodically broadcasted in every 100-300 ms providing an opportunity to adversaries for accessing critical information and easily tracking vehicles. Moreover, existing methods such as RPCLP, EPCS and MODP for attaining location privacy in mix-zones environment have severely suffered due to large number of pseudonym-changes. To cope with these issues, we presented a Dynamic Pseudonym based Multiple Mix-zones (DPMM) strategy to acquire the highest level of accuracy and privacy. The concept of executing dynamic pseudonym change has been forwarded with respect to pseudonyms, velocity and direction of moving objects. We performed our simulations by using one SUMO simulator and analyzed results compared with existing pseudonym-changing techniques. Our simulation results outperformed various existing techniques and provided better results for achieving high privacy rate, requiring small number of pseudonym-change as well as providing best performance.

✉ Imran Memon
imranmemon52@zju.edu.cn

[1] College of Computer Science, Zhejiang University, Hangzhou 310027, China

[2] Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of China

[3] School of Economics and Mangement, Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of China

[4] University of Electronic Science and Technology of China, Chengdu, China

Keywords Road network · Multiple mix-zones · Location privacy · Location based services · Dynamic pseudonym

1 Introduction

The advent of mobile communication and ubiquitous computing has extended opportunities for users to make life easier by accessing vast information through location based services. However, accessing these services may expose users to threat of information disclosure [47]. The existing infrastructure enable mobile applications to track an entity's position and reveal statistical information based on his location. A wide range of mobile applications provide services including entertainment, health, navigation, and traffic management. These services are accessed on regular basis which is a constant threat for location privacy of a user. Personal data privacy has always been a critical problem and due to expansion of location based services, an adversary can easily track a user's location on basis of information disclosed. As a consequence, location privacy of the user becomes a challenge. The private information of a user, that has been recorded during his visit to a hospital, library, and social networking website or while driving on a road becomes an invasive catalogue of data.

Location privacy of vehicle networks has become a debatable topic in recent years. Road traffic activities are one of the most important routine activities worldwide [48]. Therefore, trustworthiness of data and position is an indispensable aspect to consider for preserving user privacy. The concept of mix-zone has been proposed by Beresford and Stajano [8] in order to tackle the problem of location privacy in traffic aware applications that explain a mix-zone as an area in which a user can alter pseudonym without being tracked by antagonists. It assists in anonymizing identity of user so that an attacker may not easily get access to user's real identity. Despite, it still remains a strenuous task to achieve desired level of protection by using a single mix-zone. In order to overcome this hurdle, a concept of multiple mix-zones is proposed to cope with problem of identity correlation over multiple mix-zones involved in a user's trajectory [41]. Vehicle Ad-hoc Networks (VANET) is the type of network which consists of vehicles having wireless devices known as On Board Units (OBU) which allow communication between multiple vehicles. This aids in generating a very discrete information such as position, speed and direction during communication [57]. Consequently, it gives opportunity to any malevolent adversary to track user and cause harm. In order to encounter this problem, regular variations in pseudonyms are indispensable to ensure privacy. A lot of work has been done in this area. In [64] a pseudonym changing scheme has been presented which is based on a number of neighbor vehicles in VANETS. Author has proposed a validation protocol based on vehicle pseudonym for smart transport system but author does not explain pseudonym communication mechanism [25]. A new scheme is designed based on a security mechanism which is known as periodic pseudonym change, in which two approaches are proposed [2]. First approach suggests a concept of central authority, where every vehicle asks for a new pseudonym after passing of time "t". According to second approach, a new pseudonym is generated by each vehicle after time "t". Moreover, each approach is evaluated on bandwidth used and on speed of vehicle. This concept implies that posted road speed is used. Whereas, in real scenario, it is contrary because vehicles travel at different speeds and few of them travel at posted speeds. In order to tackle this problem, we have based our approach on continuous change in pseudonym on road network inside as well as outside mix-zones [3, 7, 39, 44, 55, 66].

In the last decade, various pseudonym changing techniques for the protection of location privacy in VANETS have been proposed [11, 19, 41, 43, 72]. This can be achieved by changing the identifier of a target vehicle called the pseudonym that is chosen randomly. This mechanism is performed by location server, therefore, by executing pseudonym change, the services from main server will be disturbed which is the cause of overhead in the network [10, 46]. Generally, less than 5 s are required to complete the connection [68]. However, in order to design a better location privacy protection approach, factors like high security level along with number of pseudonym-changes are to be considered which are of significant importance. Despite, most of current pseudonyms changing mechanism have ignored this crucial aspect. In this research, researcher has aimed to design a pseudonym changing scheme to reduce number of variations made in pseudonyms, simultaneously, achieving a high level of location privacy. Furthermore, author suggests that general standards for executing pseudonym change comprise of three important factors including life of pseudonym, speed of vehicle, and direction of a vehicle movement. On the basis of this study, an attacker may get distracted if pseudonym is changed but the problem persists because, if a single vehicle changes its pseudonym, it can be tracked easily by an attacker. In order to cope with this problem, another idea is proposed to achieve several variations in pseudonyms inside a mix-zone [16]. It is further explained that a mix-zone can be expressed as the area in which various vehicles can alter their identification at the same time. According to the researcher, only when multiple vehicles are in the mix-zone, the change in pseudonym may occur. On the other hand, an attacker can easily discover mix-zones because, mix-zones are mostly, statically determined [16, 41]. So, this concept led the researchers to explore the idea of dynamic mix-zone [19, 43, 72] that emphasizes on pseudonym changing techniques which are based on dynamically determined mix-zones. In [17] game theory approach has been proposed for non-cooperative location privacy. In this approach, selfish-vehicles alter their pseudonyms when they have maximum payoff but author has failed to explain the consequences when few selfish-vehicles do not change their pseudonyms if they have achieved satisfactory level of location privacy. As a result, vehicles whose pseudonyms have expired may not find enough available vehicles to exchange their pseudonyms. This adversely affects vehicles which are in need of location privacy. Based on the above analysis and limitations of existing work, we proposed a protocol that will generate some inducement for vehicles to change their dynamic pseudonyms inside as well as outside a mix-zone.

Our main contributions are as follows:

(i) We introduced a reputation-based method named as Dynamic Pseudonym Multiple Mix-zone (DPMM) which gradually encourages each vehicle to change pseudonym dynamically inside as well as outside a mix-zone over the road network. Moreover it comprise of various parameters like distance, velocity and difference in vehicle's trend of movement. We also proposed a novel scheme that ensure privacy for road networks and defend vehicles against various attacks.

(ii) We proposed a new reputation-based dynamic pseudonym-change protocol for location privacy protection where each vehicle's verification is carried out at the reported server.

(iii) Simulation results revealed that proposed technique outperforms existing techniques and provides better results in terms of acquiring high rate of protection as well as, reduced number of changes required in pseudonyms.

(iv) We verified the importance of our technique by using real world mobile vehicle traces and have made comparisons with certain existing methods. Our analysis has revealed that the proposed method has outperformed existing methods especially in terms of privacy preservation, dynamically changing pseudonym, packet delivery ratio, life time of pseudonym and several other factors.

2 Related work

Modern location based systems (LBS) are termed as mobile location services, wireless location services and location aware applications. They may also be termed as software applications, location aware technologies, mobile communication systems and handheld mobile devices [72]. Location based systems are also used by a satellite positioning technology which locates the position of object and people such as Global Positioning System (GPS) and Geographical Information System (GIS) which comprises of databases filled with physical location data. In [80] LBS is generally defined as an application, which provides the information services related to and reliant upon the location of the entity or location information concerned with the traveler. In this context, the author has ignored indoor technologies like Bluetooth, RFID and Wi-Fi and restricts the research to outdoor location based systems where information regarding positioning can be measured by the mobile network or some other device so as to determine the location of mobile device. Henceforth, in order to ensure the privacy of location, pseudonyms are created in an already defined manner. It disables invader to connect with the current pseudonym of a vehicle and the formerly generated pseudonym used by the same vehicle. On the contrary, the alteration in pseudonyms does not produce the robust solution because most often, the vehicles may have dissimilar trajectories and speed. Thus, an assailant can calculate the position using physical correlation. In order to avoid such obstacles, another technique is proposed in [29], where the vehicle remains silent for specific time inside mix-zones after which it will change pseudonym in close time by using minimum K-1 other users .This concept gave researchers a new direction towards fixed mix-zone concept which on the contrary, is confined to be implemented only at path crossings [12, 18, 61, 70].

Fixed mix-zones portray certain general features including zones which are applied at pre-decided positions, and the traffic that enters the system change their pseudonyms (mostly intersections are considered for mix-zones). Moreover, vehicles inside the fixed mix zone, have to remain silent and all communication applications remain passive or disconnected. An important conflict that arises here is that when the pseudonym of a vehicle expires before it enters into the mix-zone, the vehicle may transmit the security message using its previous pseudonyms or it will change to the new pseudonyms. To avoid such ambiguity, the concept of cryptographic fixed mix-zones is implemented at intersections of roads [19]. By implementing the concept of cryptographic fixed mix-zones, message would get encrypted. So, the vehicles inside this area can transmit security information which is contrary to the idea of the fixed mix-zones. It makes the concept of cryptographic fixed mix-zone unfeasible. So, another important addition was made by the Sampigethaya, who proposed that a group of vehicles can be led by a head-vehicle, giving the opportunity to the other automobiles to stay quiet for a long period of interval [4]. It was observed that this idea failed to achieve desired output in time sensitive security applications, resulting in very high end-to-end delay. Apart from that, if head-vehicle is captured by some attacker, then the security and privacy of all other vehicles inside that group will also be at stack.

Therefore, another concept of user-centric approach named as swing and swap was put forward which has amplified the secrecy by allowing vehicles to lightly coordinate their updates by altering their velocity [40]. However, alteration in vehicle's velocity like that of its path is not adequate. The time duration required for broadcasting a security message consists of a few microseconds, being too short to be regarded as a silent period. So, the method described in [40] fails not only because the pseudonyms updated vehicles stay quiet for a small time but also because this approach is impractical when automobiles are on highway or on a single road. The basic idea proposed by the author is that the vehicle v and its neighbors have to change their pseudonyms until there must be at least K-1(K > =1) vehicles [43]. Hence, in the above defined scenario, when vehicles v's neighbors are in small number, such as, in the case of a low traffic road, this approach becomes impractical to apply or provides insufficient security level if implemented. A more robust concept based on dynamic mix-zone is given in [84] to avoid this obstacle. In this case, every entity can estimate its defined mix-zone by using a trusted intermediary. In the above defined scenario, it is not compulsory for every vehicle to stay silent in the mix-zone so, it can be implemented for a promising output. But, this approach has also its limitations due to the fact that, a self-centered vehicle may not cooperate during pseudonym change because of large overhead occurring in the process of pseudonym change [5, 33, 34, 50, 52].

A lot of work has been done, which focuses on self-centered and selfish vehicles in the mix-zone [9, 16, 20, 30, 43, 63]. But as a matter of fact, these techniques for securing confidentiality are way too expensive and troublesome. To address such issues, another technique has been proposed in [30]. On the basis of game theory, the author analyzed the location of mixed zones in the optimal regions and has also assumed the occurrence of local antagonist. He further anticipated a conclusion about the optimum behavior of the vehicles and the attacker. Lu et al. [43] also based his study on game theory inferring that vehicles use pseudonyms because of the characteristics of social places. However, both approaches failed to consider vehicle's varying location privacy. Therefore, building mix-zone for vehicles by using cryptographic approach, has been proposed in [62]. It is moreover, suggested to construct cryptographic mix-zones by placing different road side units (RSU) at the points where extraordinary traffic density is observed. Once cryptographic mix zone has been approached by the vehicle, RSU would assign a symmetric key to the vehicle. As long as the vehicle remains inside this mix-zone, entire communication remains encrypted and an antagonist may not alter data in the message. Vehicles inside the mix-zone will communicate with the vehicles outside the mix-zone being in direct range and may decrypt the messages. Hence, the messages may also be exchanged and decrypted by the vehicles. At the same time, vehicles will change pseudonyms while staying inside the mix-zone. A further research in this area led to an infrastructure less approach which has been presented against the global adversaries in [51, 65]. In this approach, vehicles are grouped together for a short period of time along with maintaining the silent period. In this scenario, all the vehicles remain silent except for the group leader which broadcasts information. Moreover, the remaining vehicles will introduce the period of silence, exposing less information for the adversary, when vehicles change their pseudonyms [14, 21, 38, 42, 69, 71].

While using pseudonyms, we can disconnect the location data from a particular user. In [37] the idea of dynamically changing pseudonyms in a mixed zone was initially introduced, where multiple users meet, restricting an antagonist from connecting multiple pseudonyms of the same user. But, this idea is only applicable when antagonist has just a limited view of user's movement and analyzes pseudonyms of vehicles while entering and exiting the same mix zone. In [26] authors proposed the path alarming mechanism that adds certain noises to actual location data so that every user can design different possible path by swapping their pseudonyms unless they meet at the same place. This technique, however, may not consider an antagonist's outside information that can connect each user with a particular location. In [24] the concept consists of location anonymization and is being used by several other researchers [6, 22, 23, 58]. Recently, research has been conducted on location anonymity that focuses on road networks [54, 81]. The concept of Xstar has been offered in [81] which proposed concealing the locations based on QoS requirements and road network privacy. It maintains the stability among the processing cost of unidentified query and the attack resilience of the performed safety. In [54] Casche cloak algorithm has been proposed. In this approach, cache prefetching is used to conceal the actual position of an entity by inviting the location built data over a known path. This algorithm is based on location cloaking and it is not suitable when user asks multiple inquiries along with their movement and may not be implemented where exact point location of mobile users is required [30]. The concept of mix zones to pseudonym changes has been presented in [72] and the construction of road intersection mix-zone concept has been given in [16, 43]. In [17], construction for optimal adjustment of mix zone in a road network has been debated. So, it reflects that in all these mix-zone techniques, most of approaches have followed the concept of circular zone or rectangular zone, and their design methodology is unable to answer the problems related with attacks due to timing and transition in the design mechanism. Therefore, in our research, the problem of confirming an unpredictable value of anonymity has been taken into account, and at the same time, statistics regarding user arrival and other aspects in the road networks have also been considered [31, 32, 35, 36].

3 System model and scenario

3.1 Overall idea definition

We proposed a Dynamic Pseudonym Multiple Mix-zone model (DPMM) for mobile travelers over Road networks. In this model, we allow vehicles to change their pseudonyms dynamically when they enter a mix-zone. We have further placed the reported servers (RS), which will permit communication between road side unit (RSU) and vehicles. Because, vehicles are connected to reported server (RS); they may change pseudonyms even when they are outside a mix-zone. We proved our results by performing experiments and using mathematical models for probability changing pseudonyms and time & speed model as explained in section 3.4 and 3.5 respectively.

3.2 Assumptions

In this research model, we proposed a protocol and assumed that each vehicle has a unique ID (identity information in road network). This ID is only shared with reported server (RS). We also assumed that RS_1, RS_2… RS_n all are connected to main RS servers and main RS verify each unique ID information and provide information to multiple reported server (RS), which is used for requesting a change in pseudonyms when vehicle travels inside or outside a mix-zone. It is further assumed that every vehicle is authenticated by a private or public key. This key allows a vehicle to acquire its pseudonym and its RS information from reported server. Moreover, mix-zone and reported server are trusted entities, while RSU is not a trusted entity. Under such circumstances, a reported server is responsible to control vehicles. RS information and public keys, both are available at reported server. Reported server broadcasts a public pseudonym for each vehicle which comes under its range or detected over road network. The availability feature of RS is almost perfect. Additionally, it has the information of RS private IDs and encrypted information of public keys associated with every vehicle. Thus, RS will acquire a vehicle's public key and frequently update it.

3.3 Model description

(1) In our first approach, we proposed that every vehicle gets associated with RS, where RS allocates a virtual identity and a secret pseudonym. The virtual ID (dummy identity of vehicle user instead of using real identity) is a node identity for vehicle user which is 128-bit address used for both node identity and locator. The virtual ID is pre-defined and randomly assigned by the main reported server. This ID is permanent and thus, no longer bound to the main reported server and/or locations. Once a vehicle receives a virtual identity and a private pseudonym, it will resend it to reported server which, in turn, broadcasts this new generated RS information. Hence, vehicle encryption includes public pseudonym, its virtual identity and timespan of RS information. Time span of RS information can be defined as time which is required for a vehicle to travel at a regular speed to cover distance between two reported servers. During this process, vehicle sends its virtual identity to RS, before its certificate expires. RS will resend newly generated private pseudonym to vehicle when it receives virtual identity of vehicle, while at the same time, it will update reported server regarding the vehicle's information. Hence, reported server will broadcast certificate. In this approach, vehicles on road are identified by their virtual identity while pseudonyms allow them to communicate. However, in this approach only RS will communicate with road side unit (RSU) as depicted in Fig. 1. The number of road side unit (RSU) may communicate with multiple reported servers which are installed within the infrastructure. Therefore, the capacity of multiple reported servers and number of vehicles to communicate with an infrastructure depends upon the radio coverage of existing RSUs in the nearby area. The bandwidth required to send a request and receive response of pseudonym will be analyzed in section 3 and its parameter is defined in Table 1.

In Fig. 2, related steps are offered as follows:

1: RS broadcasts periodically its public key.
2: Vehicle sends to RS a ERpbKey(Vid) message.
3: RS sends to the applicant vehicle a EV$_{\mathrm{id}}$(V prpseudo + V $_{\mathrm{vid}}$) message.
4: RS sends to RSU aV RS inforamtion message.
5: RSU broadcasts V RS inforamtion message.
6: Vehicle sends a EV id(V $_{\mathrm{vid}}$) message to the RS.
7: RS delivers a EV $_{\mathrm{id}}$(V' prpseudo + V' vid) message to the vehicle.
8: RS sends to RSU a V' RS inforamtion message.
9: RSU broadcasts V' RS inforamtion message.

(2) In our second approach, we proposed that every vehicle has both its private and public key. As the vehicle acquires RS public key, it will be authenticated on road network by encrypting its private keys and public keys with RS public key. Hence, vehicle pair keys (i.e. private/public) get registered with RS and in turn, RS will send a set of information to vehicle by encrypting them with vehicle

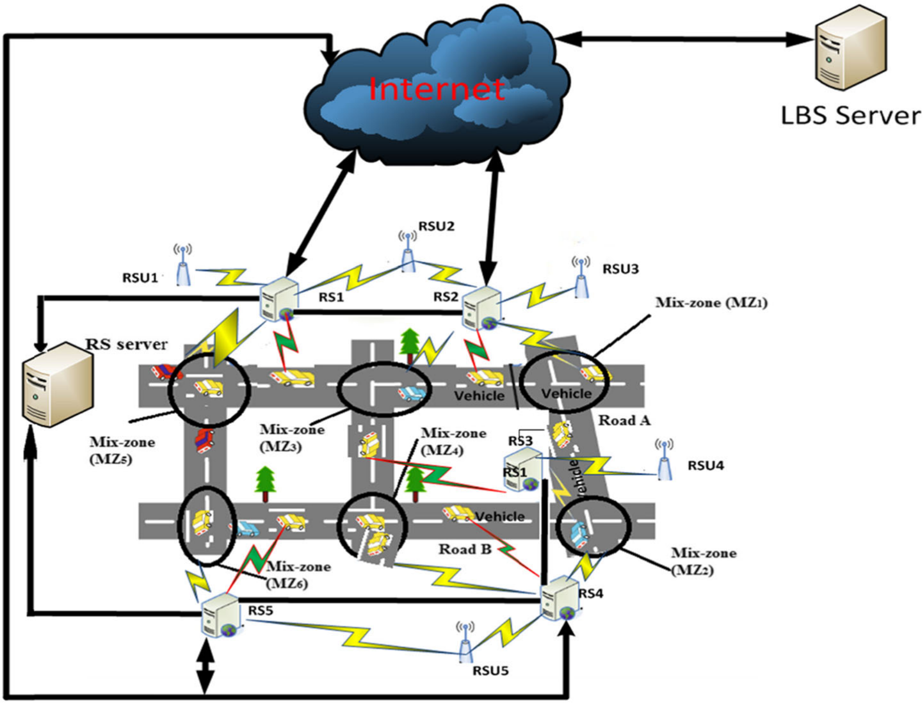


Fig. 1 System model dynamic Pseudonyms changing

public key. This information contains a message that allows vehicles to create their private pseudonym and certificate. So based on this, when a vehicle receives a set of information, it creates a certificate and a private pseudonym. Once it is done, RS information will be broadcasted. As soon as RS information expires, it will generate a new private pseudonym that will be broadcasted. Pseudonyms are the only way to identify vehicles by using this approach. However, vehicles in second method are free to communicate their private pseudonyms and certificates, once they have been validated by RS. Figure 3 describes different steps of the technique 2. The steps are as follows:

1: RS broadcasts periodically its public key.
2: Vehicle sends to RS a ERpbKey(V prKey + V pbKey) message.
3: RS sends to the applicant vehicle a EV pbKey(V pseudRsinf) message.
4: Vehicle generates its private pseudonym and RS information.
5: Vehicle broadcasts its new RS information.
6: Vehicle updates its private pseudonym and new RS information.
7: Vehicle broadcasts the new RS information.

The RSUs are scattered equidistantly to measure expiration time of certificates and private pseudonyms. Consider “d” as a distance between each road side unit and communication range of each road side unit. Moreover, maximum and minimum speed on road are represented by V_{max} and V_{min}, respectively. It is assumed that there must be at-least two vehicles which may travel at an average speed. The main

Table 1 Notation description

Notation	Description
V_{id}	Vehicle's identity.
V_{pKey}	Vehicle's private. Key
V_{pbKey}	Vehicle's public key.
RS	Report server
Vpr	Vehicle's private pseudonym.
V_{vid}	Vehicle's virtual identity.
V pseudRSinf	Vehicle's pseudonym and Report server information.
RpKey	RSU's private key.
RpbKey	RSU's public key.
ERpbKey(V_{id})	Asymmetric encryption function at encrypts the vehicle identity with RSU public key.
EV $_{id}$(Vpseudo + V_{vid})	Symmetric encryption function that pseudonym and its virtual identity with the real identity of the vehicle.
ERpbKey(VprKey + V pbKey)	Asymmetric encryption function public key with RSU public key.
EVpbKey(V pseudRSinf)	Asymmetric encryption function that encrypts the set of information (which permit at the vehicle to generate its pseudonym and certificate) with its public key
Br(V $_{RSinf)}$	Broadcast the vehicle certificate.
EVid(V_{vid})	Symmetric encryption function that encrypts the vehicle virtual identity with its real identity.
EV $_{id}$(V' prpseudo + V'_{vid})	Symmetric encryption function that encrypts the new private pseudonym and virtual identity of the vehicle with its real identity.
V'_{RSnew}	Vehicle's new RS information
Br(V'_{RSnew})	Broadcast the new RS information

goal of our approach is to allow at least two vehicles to acquire pseudonym on road during same time interval. It is denoted by $V_m = (V_{max} + V_{min})/2$. The ratio determined between distance "d" and "V_m" will be the expiry time "t" of certificate and private pseudonym, which is represented by $t = d/V_m$. The communication range of each road side unit is equal to "d" as mentioned previously. Therefore, any vehicle at any speed can communicate with at least one road side unit and is allowed to change its pseudonym at least once while on the road as shown in Fig.4

(i) t_0: subnet enter (come-in) time,
(ii) t_3: subnet leave (come-out) time,
(iii) $t_s = t_3 - t_0$: subnet residence time,
(iv) t_1: current observation time,
(v) t_2: new pseudonym update time,
(vi) T_r: pseudonym change interval.

We model the privacy exposure time with the timing diagram, and develop the optimal pseudonym change algorithm. After the observation starts at t_1, a pseudonym is changed (updated) either at t_2 by a periodical pseudonym change or at t_3 by a handover.

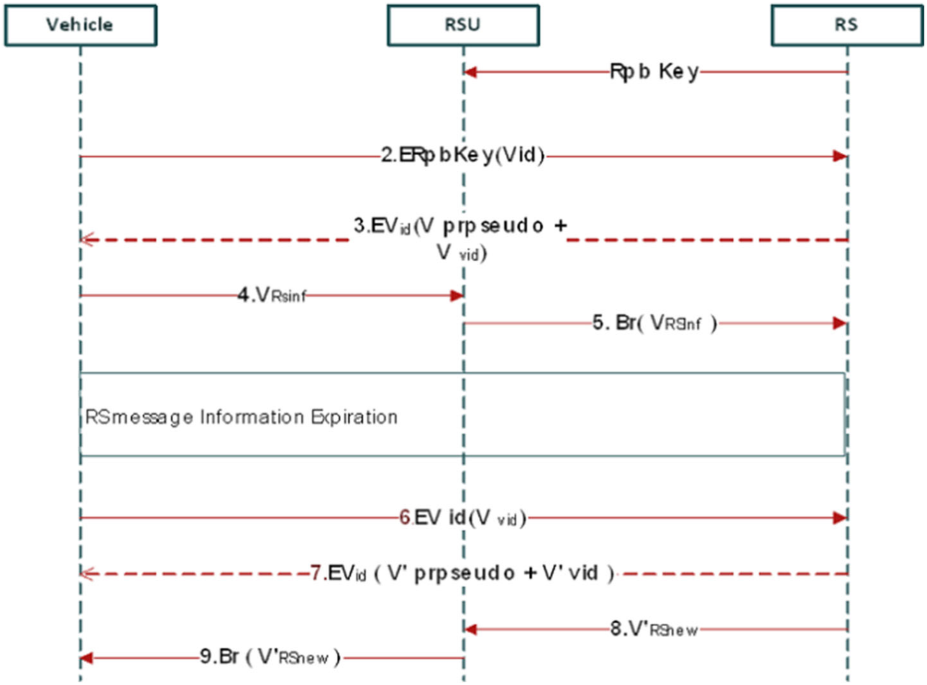


Fig. 2 Interactions first technique main steps

Therefore, the privacy exposure time z is given by

$$z = \min\{z_1, z_2\} \tag{1}$$

Where $z_1 = t_2 - t_1 (0 < z_1 < T_r)$ and $z_2 = t_3 - t_1 (0 < z_2 < \infty)$.

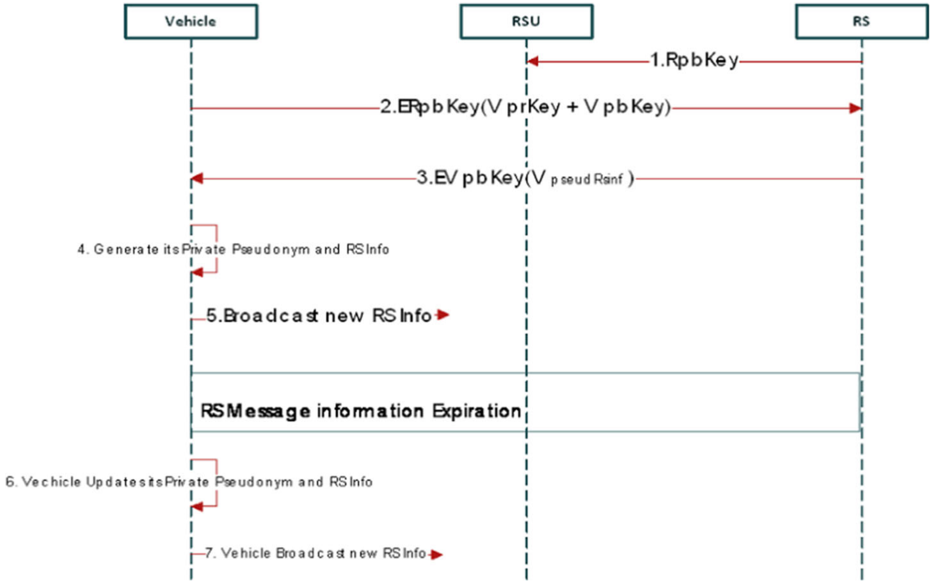

Vehicle
RSU
RS
1.RpbKey
2.ERpbKey(V prKey + V pbKey)
3.EV pbKey(V pseud Rsinf)
4. Generate its Private Pseudonym and RS Info
5.Broadcast new RS Info
RS Message information Expiration
6. Vechicle Updates its Private Pseudonym and RS Info
7. Vehicle Broadcast new RS Info

Fig. 3 Interactions second technique main steps

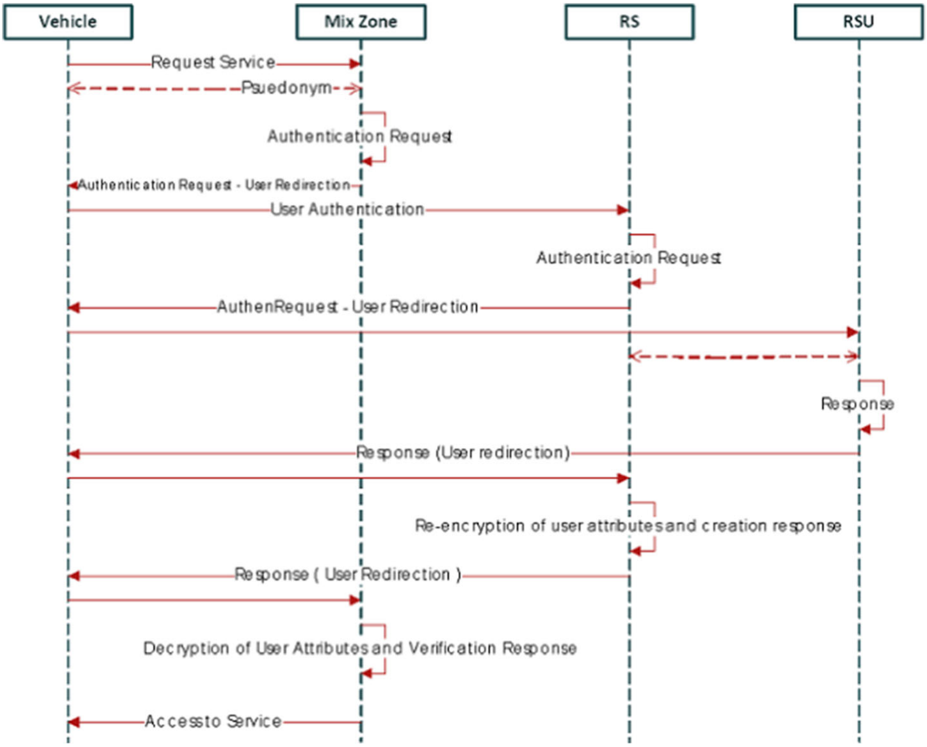

Vehicle
Mix Zone
RS
RSU
Request Service
Psuedonym
Authentication Request
Authentication Request - User Redirection
User Authentication
Authentication Request
AuthenRequest - User Redirection
Response
Response (User redirection)
Re-encryption of user attributesand creation response
Response (User Redirection)
Decryption of User Attributes and Verification Response
Accessto Service

Fig. 4 Communication scenarios

Then, the probability density function (PDF) of z is given as:

$$f(z) = f_1(z)\int \infty z f_2(t)dt + f_2(z)\int \mathrm{Trz} f_1(t)dt \tag{2}$$

where $f_1(z)$ and $f_2(z)$ are PDFs of z_1 and z_2, respectively.

Now, we need to find proper distributions for z_1 and z_2. The pseudonym change interval Tr is a constant and $t1$ is a random observer time epoch. Therefore, $z1$ follows a uniform distribution in $[0, T_r]$ and thus $f_1(z)$ is obtained as:

$$f_1(z) = 1 \tag{3}$$

On the other hand, if the subnet residence time ts follows an exponential distribution with mean of $1/\mu s$, $f_2(z)$ is calculated as:

$$f_2(z) = \mu se{-}\mu \tag{4}$$

Then, the PDF of z, (z), can be expressed as:

$$f(z) = f1(z)\int \infty z f_2(t)dt + f_2(z)\int T_r z f_1(t)dt = 1T_{re}-\mu sz + \mu se-\mu sz_1 T_r(Tr-z)$$

From (2), the Laplace transform of (z), $f*(s)$, can be obtained and the expected privacy exposure time, $E[z]$, can be obtained from $E[z] = (d/ds)f*(s)|s{=}0$. Suppose a vehicle generates packets with rate λp (packets/s). Let N denote the expected number of packets influenced by the privacy exposure. Then, N is calculated as:

$$N(T_r) = \lambda p \times E[z] \tag{5}$$

Intuitively, (T_r) increases with the increase of Tr. Therefore, the optimal value of T_r can be obtained from the following problem: maximize T_r subject to

$$N(T_r) \leq \Theta \tag{6}$$

3.4 Probability changing the pseudonyms

In this section we are going to calculate how probability of changing pseudonyms can be calculated, we have proved our results by simulations and using mathematical equation as explained below.

Φ(v), is the probability that v vehicle is connected to RS and passed through number of mix-zones during the same interval.

Ψ(Pv) is the probability that a vehicle changes pseudonym inside and outside mix-zones while travelling on a road it has chosen to have pseudonym (Pv).

The number of mix-zones in the road system is given by graph and edge (G,E).

The maximum number of vehicles connected which pass through mix-zones on the road system are denoted as mix-zones_r and dynamic pseudonyms are denoted as mix_rdpvt. Here, we define:

G ([PV1, ..., PVC]) to be the set of dynamic pseudonyms change[PV1, ..., PVC] in the graph G, E.

$$\mathrm{G}\ ([\mathrm{PV}_1, \ldots,\ \mathrm{PV}_\mathrm{C}]) = \left\{\mathrm{m}\middle|\mathrm{m} = \left\{\middle|[\mathrm{e}_1, 1 \ldots \mathrm{e1}\ \mathrm{PV}_1]; [\mathrm{e}_2, 1 \ldots \mathrm{e}_2,\ \mathrm{PV}_2]; \ldots; [\mathrm{ec}, 1 \ldots \mathrm{ec},\ \mathrm{PV}_\mathrm{C}]|\right\} \wedge \mathrm{ex}, \mathrm{y} \in \mathrm{m} \Rightarrow \mathrm{ex}, \mathrm{y} \in \mathrm{E}\right\}$$

So, the probability P of a particular vehicle connected to RS is shown as:

$$P = \sum_{v \in 0 \ldots max-\mathrm{zones\_}r} \Phi(v) \times \sum_{\substack{Pv = [PV1, \ldots, PVC]\big) \\ \forall i.Pv_i < \ are\ mix\_\mathrm{rdpvt}}} \prod_{PV1,\ldots,PVC \in Pv} \times \sum_{g \in G(Pv)} \frac{\big|p\big| p \in g \wedge \forall_{e \in\ p\ f_g\ (e)=1}}{\big|g\big|} \tag{7}$$

3.5 Time and speed

In this section we are going to calculate time and speed of vehicle at multiple time and location when vehicle enter inside mix zone and leave mix zone at some time interval.

For a mix zone model, let's assume Ŝi and Ŝj represent the variables related with the speed of vehicles i and j respectively. The speed in this scenario, follows the Gaussian distribution whereas, the variables Ŝi and Ŝj are assumed to be normal variables. Let t be the time of user at which vehicle exits and is assumed to be t-out (i). However Pi' → j is the probability of exiting vehicle i's j and on the other side, Pi' → i is the probability that the exiting vehicle is i. So, we may assume that if one of these probabilities differs from the other, it will have more chance that adversary will match old pseudonym with new pseudonym [28, 45].

Let's assume t and t + 1 be the time interval of the vehicle j when it exits the mix zone and P (j, t) represent its probability. So, P (j, t) is equal to the probability that a vehicle j utilizes time in between

$(t - t_{in}(j)) to (t + 1 - t_{in}(j))$ to cover the distance $d_i(j)$.

So $v1 = \frac{d_i(j)}{(t - t_{\mathrm{in}}(j))}$ to $v2 = \frac{d_{i(j)}}{(t+1-t_{\mathrm{in}(j)})}$ is the distance with an average speed that vehicle J has to travel during the time interval t to t + 1. Hence it can be written as:

$$\mathrm{P(j,t)} = \int_{v2}^{v1} \hat{S}j(v)dv \tag{8}$$

At the same time,

$$\mathrm{P(i,t)} = \int_{v2}^{v1} \hat{S}i(v)dv \tag{9}$$

Where $v1 = \frac{d_i(j)}{(t - t_{\mathrm{in}}(j))}$ to $v2 = \frac{d_{i(j)}}{(t+1-t_{\mathrm{in}(j)})}$

We have

$$\mathrm{P}\left(\mathrm{i'}, \mathrm{t}\right) = P(i,t) + P(j,t) \tag{10}$$

Hence,

$$W_{\tau}^{j} = -\sum_{d=1}^{N_{\tau}^{j}} P_{d \downharpoonleft b} log_2 P_{d \downharpoonleft b} \tag{11}$$

Change Pseudonym

$$\sum_{w=0}^{x-1} P\{N_U^V = w\} P\left\{N_V^Q = x-1-w\right\} P_{V_w} P_{q_{x-1-w}} \tag{12}$$

The above equation represents the probability sum of all the X-1 neighbors of the target vehicle changing their pseudonyms with the target when V_w *and* Q_{x-1-w} meets the basic condition:

$$\mathrm{P\{|At| = x\}} = \sum_{w=0}^{x-\ 1} P\{N_U^V = w\} P\left\{N_V^Q = x-1-w\right\} \tag{13}$$

So, we can also say that when up_m is greater than zero, vehicle i will always slater its cost to wj such that wj < $\left(\frac{up_m d_j}{up_m} + 1\right)$

Therefore, vehicle j can vigorously alter its pseudonym at the mix-zone. So, the location privacy of vehicle J can be stated as:

$$lpg_j = -\frac{d_i}{up_m + 1} - (-d_i) = \frac{up_m}{up_m + 1} . d_j \tag{14}$$

Finally, the feasibility of the PCS strategy in practice is given by.

1. F_i and F_{i-1} is the distance between two vehicles and it has been denoted by Y_i^L. Variables $Y_1^L, Y_2^L, Y_3^L \ldots\ldots Y_i^L$ are independent and identically distributed, and their common probability density function is $f(x) = \measuredangle e^{-\measuredangle x}$.
2. The distance between the left vehicle Li and the target T has been denoted by S_i^L. The probability distribution function of S_i^L is given as:

$$P\{S_i^l \le x\} = 1 - e^{-\lambda x}\left[1 + \lambda x + \ldots + \frac{(\lambda x)^{i-1}}{(i-1)!}\right. \tag{15}$$

3. The number of vehicles inside the mix-zone having distance r is denoted by V(r) whereas, the probability of the number of vehicles inside mix-zone having distance r is denoted by

$$P\{V(r) = i\} = \frac{(\lambda r)^i}{i!}e^{-\lambda x} \tag{16}$$

So, now we can calculate the size of anonymity set of the target vehicle in CPN scheme, which is given by:

$$P\{|Ar| = z\} = 2 \sum\nolimits_{n=0}^{K-z} P\{N_T^L = z-1\}P\{N_T^R = n\}P_{l_{z-1}}(1-P_{R_n}) + \sum\nolimits_{m=0}^{z-1} P\{N_T^L = m\}P\{N_T^R = z-1-m\}P_{t_m}P_{R_{z-1-m}} \tag{17}$$

In some situations, an attacker may monitor a subset $E_n = \{E_1, E_2, E_3, \ldots .E_n$ which is used to identify a vehicle during PC process. Let's assume $S_0 = (u_1, u_2, .. u_n) and\ S_1 = (w_1, w_2, \ldots w_n)$ are the distance vectors of two vehicle's PC process being observed by an attacker. So, the similarity between S0 and S1 can be re-written as:

$$cos(S_0, S_1) = \frac{S_0.S_1}{|S_0|.|S_1|} = \frac{\sum_{i=1}^{n} x_i \cdot y_i}{\sqrt{\sum_{i=1}^{n} x_i^2 \cdot \sum_{i=1}^{n} y_i^2}} \tag{18}$$

When S0 and S1 are same, then $\cos(S_0, S_1) = 1$, because of the monitoring inaccuracy. If $|1 - \cos(S_0, S_1)| \le \varepsilon$, so for some small confusion values $\varepsilon > 0$. Therefore, these two PC processes would be vague to the attacker. Thus, in order to implement high location privacy, vehicle should take many vague PC processes simultaneously.

When vehicles enter the mix-zone during the time period Ts, we may write the equation as:

$$\begin{aligned} Q_r[Y = y] &= \int_{t=0}^{\infty} Q_r\ [Y = y \mid T_s = t] f(t)dt \\ &= \int_{t=0}^{\infty} \frac{(\lambda t)^y}{y!} e^{-\lambda t} f(t)dt \\ &= \left(\frac{\lambda^y}{y!}\right)\int_{t=0}^{\infty} t^y e^{-\lambda t} f(t)dt \\ &= \left(\frac{\lambda^y}{y!}\right)\left[(-1)^y \frac{d^y f^*(s)}{ds^y}\right. \\ &= \frac{\mu\lambda^y}{(\mu+\lambda)^{y+1}} \end{aligned} \tag{19}$$

So, the Laplace transform $f^*_{\check{e}}(\check{e})$ becomes:

$$f^*_{\check{e}}(\check{e}) = (\frac{\text{Ł}}{\text{Ł}+\mu}) \tag{20}$$

Hence, S-anonymity can be re-written as:

$$\begin{aligned} ASS &= \frac{\leftthreetimes}{\mu} - \sum_{x=1}^{\infty}\{\{\sum_{y=1}^{x} y \binom{x}{y}\left(\frac{\text{Ł}}{\text{Ł}+\mu}\right)^{y}\left(1-\frac{\text{Ł}}{\text{Ł}+\mu}\right)^{x-y}\}\times[\frac{\mu\leftthreetimes^{x}}{(\mu+\leftthreetimes)^{x+1}}]\} \\ &= \frac{\leftthreetimes}{\mu} - \sum_{x=1}^{\infty}\{x.\left(\frac{\text{Ł}}{\text{Ł}+\mu}\right)\times[\frac{\mu\leftthreetimes^{x}}{(\mu+\leftthreetimes)^{x+1}}]\} \\ &= \frac{\leftthreetimes}{\mu} - \frac{\text{Ł}\mu}{(\text{Ł}+\mu)(\mu+\leftthreetimes)}\sum_{x=1}^{\infty} x.\left(\frac{\text{Ł}}{\text{Ł}+\mu}\right)\times(\frac{\leftthreetimes}{\mu+\leftthreetimes})^{x} \\ &= \frac{\leftthreetimes}{\mu} - \frac{\text{Ł}\leftthreetimes}{\mu(\text{Ł}+\mu)} = (\frac{\leftthreetimes}{\text{Ł}+\mu}) \end{aligned} \tag{22}$$

3.6 Attacks in multiple mix-zones over road networks

In the following section, we shall discuss the possible attacks on the road network.

(1) Fabrication Attacks: In this type of attack, an adversary may penetrate some malicious information into the network. When appropriate entity in the network would receive unauthorized packet, it can be misled to some anonymous destination. In addition, an attacker can make this attack by transmitting false information into the network, or the sender could claim that it is somebody else. This attack includes fabricate messages, warnings, certificates, identities [67, 1, 56]. The greedy drivers fabricate messages using broadcast methods and then launch the attack by sending these messages into the network. Fabrication of the messages has two possible forms. False information about an attacker's ID, speed and location of vehicle is sent to other vehicles or RSU. Another possibility is that the attacker will present himself/herself as an emergency vehicle, so that he/she can drive at a faster speed [60]. Our system avoids this type of attack because of secure communication system architecture and RS server. Secondly, we cloak synchronization (between nodes) and IP filtering in our system.

(2) Message Suppression Attacks: In this type of attacks, an adversary might drop down some critical information or some message which is sent to the receiver or hold that information to be used for later time. In road networks, this may create a very critical issue, like the information regarding the accident may not reach to the user in time. In case of any mishap, the information regarding that incident will not immediately be propagated to the insurance authorities. These packets may hold critical information for the receiver. The attacker suppresses these packets and can use them again at another time. The goal of such an attacker would be to prevent registration and insurance authorities from learning about collisions involving his/her vehicle and or to avoid

delivering collision reports to roadside access points. For instance, an attacker may suppress a congestion warning and use it at another time so that vehicles do not receive the warning and can be forced to wait in the traffic [27, 49, 53, 73].

(3) Alteration Attacks: Adversary, in such attacks, tries to change existing information by using delaying tactics or changing the actual information about the entry of vehicle that has been communicated. In such scenario, an adversary may alter the message by informing its neighbor vehicles on the road network that the road is clear but on the contrary, the road is blocked [59, 67, 75].

(4) Denial of Service Attacks (DOS): These are very popular security threats in the communication network. In this type of an attack, the attacker acquires the control of the resources, blocking the channel used by vehicular network. This will restrict the information from arriving safely and timely at final destination. Hence, these types of attacks may hinder drivers who are dependent upon application's information. In order to avoid such circumstances, the driver may switch between multiple channels or technologies if available like Bluetooth, LTE Wifi and DSRC [15, 67, 82].

(5) Replay Attacks: An adversary attacks by repeating the communication of a message that has been received earlier. By doing this, he will take the advantage of current situation and plan some critical attacks. It does not contain sequence numbers or timestamps. As keys can be reused, it is possible to replay stored messages with the same keys to insert bogus messages into the system without any detection. Individual packets must be authenticated, not just encrypted. Packets must have timestamps. The goal of such an attack can be, to confuse the authorities and possibly to prevent identification of vehicles in hit-and-run incidents [27, 73]

4 Experiments and evaluation

4.1 Experiment setup

In this section we present detail about our simulations and experiment, it is further explained that in section 4.2 we have shown the effect of number of mix zones on dynamic change pseudonyms, moreover section 4.3 represent how delay characteristic at road intersection can be calculated, finally section 4.4 explains, how packet delivery ratio can be computed when data is being sent from one vehicle to another vehicle. Furthermore detail about SUMO simulator is given below.

SUMO is an open source, highly portable, microscopic road traffic simulation package designed to handle large road networks. Its main features include collision free vehicle movement, single-vehicle routing, multi-lane streets with lane changing, junction-based right-of-way rules, hierarchy of junction types, an openGL graphical user interface (GUI), and dynamic routing. SUMO can manage large environments, i.e., 10,000 streets. Thus, by combining SUMO, openstreetmap.org and target map, we can simulate traffic in different locations of the globe. However, since SUMO is a pure traffic generator, its generated traces cannot be directly used by the available network simulators, which is a serious shortcoming of this simulator. A widely-known vehicular traffic simulator is SUMO (for further available traffic simulators see [28, 45]. They try to closely represent the movement patterns of users. The Simulation of Urban Mobility

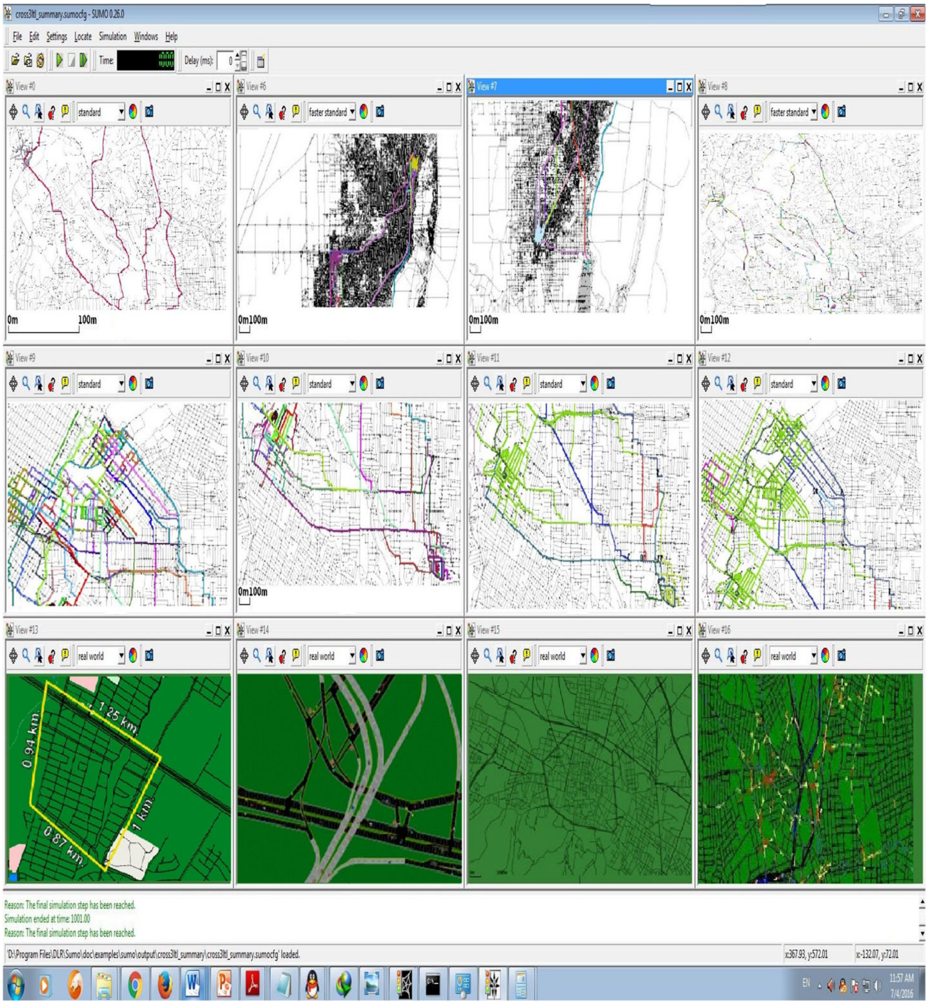
(SUMO) mobility generator supports several mobility models, such as the Krauss mobility model with some modifications to allow multi-lane behavior, and the Wagner mobility model. Mobility trace files can be generated from the Google Earth or TIGER databases. Custom (random and user) graphs are also supported, although the node movement is constrained to a grid in a random graph. The SUMO simulator generates mobility based on road networks where movements between source and destination roads are determined by a shortest path algorithm. We use and extend the SUMO simulator to generate feasible mobility traces for e-vehicles. To simulate vehicular traffic in a realistic environment, Northwest Atlanta region maps including details about street type, number of lanes, speed limitations, etc. can be imported to SUMO from geo-data sources. We evaluated our proposed method with SUMO simulator [74, 77–79] and real map Northwest Atlanta region Map is used. We have based our analysis covering a large area of 14 km × 12 km and over 10,000 vehicles moving at varying speed. The simulations have been run five times as depicted in Fig.5, moreover network parameters are set as shown in Table 2.

4.2 Performance evaluation

The simulation results shown that vehicles passing through multiple mix-zones have changed their pseudonyms dynamically as depicted in Fig. 6. Five different numbers of mix-zones and their data mechanisms corresponding to dynamically changing pseudonyms have been considered respectively. It is worthy to note here that, due to dynamically changing pseudonyms in y-axis as shown in Fig. 6 and Table 3, it is clear that DPMM is a better technique in terms of dynamically changing pseudonyms as compared to EPCS (Efficient Pseudonym Changing Schemes for Location Privacy Protection) [13], RPCLP (Reputation-based Pseudonym Change for Location Privacy in Vehicular Networks) [83] and MODP (Mix-zones Optimal Deployment for Protecting location privacy) [76]. In particular, DPMM always performs the best. As a matter of fact, pseudonym-change badly influences communication performance. If a pseudonym change interval is longer, then the privacy exposure time increases. However, if pseudonym-change interval is shorter, then overhead increases because of frequent pseudonym change. Therefore, an algorithm is required that finds an optimal pseudonym-change interval for making a balance between communication overhead and location privacy.

The average strength of location privacy for a number of vehicles, moving in SUMO simulation over Northwest Atlanta region map is shown in Fig. 7. The average strength of location privacy achieved by DPMM and EPCS is higher than RPCLP and MODP schemes, where certain selfish-vehicles inside mix-zones possessed greater location privacy thus, refusing to change their pseudonyms. The average strength of location privacy in DPMM scheme is greater when compared with other three schemes because it causes DPMM to make vehicles change their dynamic pseudonyms when they pass inside and outside the mix-zones. We conclude that average strength of location privacy maintains a certain value when numbers of vehicles increase. We further measured distance between two nodes to calculate the average location strength by using Eq. 25.

$$\mathrm{Dist}_{avg}(i,j)\lim_{N\to\infty}\frac{1}{N}\sum\nolimits_{k=1}^{N}\left|L_i(K)-L_j(K)\right| \tag{22}$$



```
Reason: The final simulation step has been reached.
Simulation ended at time: 1001.00
Reason: The final simulation step has been reached.
```

```
'D:\Program Files\DLR\Sumo\doc\examples\sumo\output\cross3ltl_summary\cross3ltl_summary.sumocfg' loaded.    x:367.93, y:572.01    x:-132.07, y:72.01
```

Fig. 5 Northwest Atlanta region map scenario using Sumo Simulation

4.3 Delay characteristics

In vehicle networks, mostly delay characteristics depend upon the road intersection. The adversary formulates road intersections with normal distributions. The delay characteristic has been investigated by using normal distribution that would use trajectory of vehicle on intersection. For example, if f is number of road segments that meets at an intersection, and we have f = 4; for vehicles arriving from u_1, their delay characteristic is represented as:

$$P_{u1}, e^{i}(t) \sim \text{Ŋ}(\mu_1, i, \sigma_1, i) \tag{23}$$

Where $I = 1\ldots\ldots$ f and e1, e2, e3 and e4 indicates the direction respectively.

Table 2 Simulation Parameters

Parameters	Value
Northwest Atlanta region Map	14 km ×12 km
Number of RSU	50
Simulation time	16.66 min
No of vehicles	10,000
Vehicle speed (m/h)	100–250
Bit rate	6Mbps
MAC protocol	IEEE 802.11
RSU Communication range	500 m
Vehicle communication range	200 m
Road Junctions	10,000
Max. transmission range	10 ms
Min. transmission range	2 ms
Routing protocol	AODV
Number of Mix-zones	500
Number of Road junctions	6831
Number of Road segments	9187
Mobility Model	Random Rnet Router

4.4 Packet delivery ratio

Packet delay is the time it takes packet to achieve the destination after it leaves the source. The average end to end delay X_{avg} can be calculated by equation given below where Wr is the emission instant of the package and Wt is the reception instant of the package.

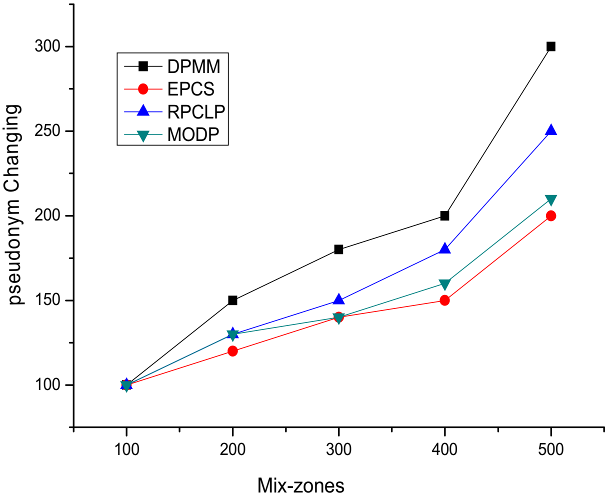


Fig. 6 Dynamic pseudonym changing

Table 3 An example dynamic pseudonym-based multiple mix-zones generation

Vehicle ID	Changing Pseudonym	Inside Mix-zone pseudonym	Key	key Time	Inside Mix-zone
Vehicle 1	2.200068e + 01 7.393244e + 00	5.820727e	59497419	2.7	2
Vehicle 2	5.820727e + 1 7.531808e + 00	1.859728e + 02	44117173	79	2
Vehicle 3	2.311176e + 01 1.408686e + 02	1.466116e + 02	34333870	5	2
Vehicle 4	5.569041e + 01 8.200338e + 01	9.181618e + 01	43909548	7	2
Vehicle 5	1.862067e + 02 1.423657e + 02	1.408686e + 02	11866731	2	2

$$X_{avg=}\sum_{j=1}^{P_r}(W_r - W_t)_{/P_r} \tag{24}$$

Location privacy inside mix-zone and outside mix-zone is represented by Ħ, however, it increases when vehicles cooperate. The strength of location privacy is directly proportional to the number of vehicles that are cooperating inside and outside mix-zone. Hence, after n number of rounds, final strength of location privacy is determined by:

$$\hat{\text{Ħ}}^{n}_{\text{Ħ}} = \sum_{y=1}^{n} W_{\tau}^{y} \;/\; A_{\tau}^{y} \tag{25}$$

The average strength of location privacy and dynamic pseudonym's lifetime is calculated for various seconds as shown in Fig. 8. The average strength of location privacy achieved by RPCLP scheme is highest as compared to DPMM and other two schemes. However, our DPMM scheme statistics still satisfies location privacy.

Figure 8 shows that the average strength of location privacy maintains a certain value with increase of dynamic pseudonym's lifetime whereas; dynamic pseudonym's lifetime has little impact on average strength of location privacy.

We performed our simulations on several vehicle densities as shown in Fig. 9. It is evident from the experiments that with a rapid increase in number of vehicles, communication range

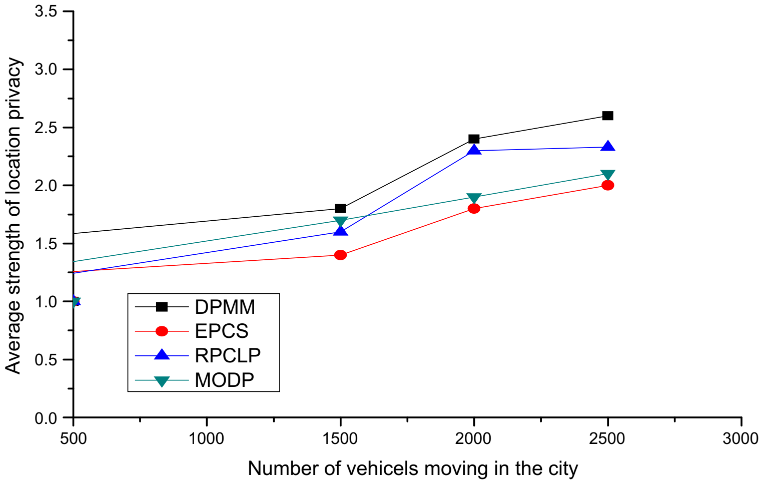


Fig. 7 Location privacy

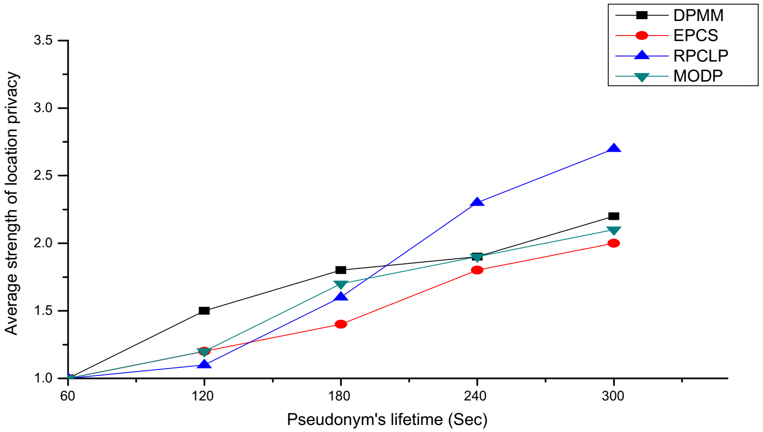


Fig. 8 Average strength of location privacy

decreases greatly as compared with the methods such as EPCS, RPCLP and MODP schemes in terms of time delay and throughput. However, with a shorter time delay, greater will be the DPMM scheme. We compared Fig. 9a, b for time delay, (c with d) for throughput and finally (e with f) for packet delivery ratio, and concluded that DPMM has outperformed EPCS, RPCLP and MODP in terms of time delay, through put and packet delivery ratio. Moreover, in Figs. 10a, b and 11a, b, we observed probability changing pseudonyms inside mix zone and outside mix zone. It is evident from the performed experiments that DPMM scheme performs better in terms of number of vehicles verses probability changing pseudonym. Additionally, as the number of vehicles increases, DPMM will give the better results as compared to other three schemes. Finally, it has been evident from Figs. 9, 10 and 11 that better results are achieved when traffic on road becomes heavier and hence, throughput can get a greater value.

We have observed that the process time will be affected by number of mix-zones and the number of target vehicles as shown in Fig. 12. It shows that as the number of mix-zones increases, processing time may also be affected. There are four scenarios that have been shown in the Northwest Atlanta region map moving in different time as 100 s, 200 s, 300 s, 400 s, 500 s and 600 s respectively. All these methods are rising up as the number of mix-zones increases. If numbers of vehicles are high then increases the size of mix-zone to improve the privacy level. Moreover, the main purpose to place multiple mix zones over the road, is the large number of vehicles inside the mix zone. As the number of vehicles increases, there are chances of congestion on the network. So, for that purpose we have increased the number of mix zones, however, by increasing the number of mix zone, we are also increasing the capability of dynamically changing pseudonym inside mix zones as well as outside the mix zone.

Existing methods for pseudonym change are not sufficient for light traffic scenario because of a very long processing time and single change pseudonym, which is unable to meet the conditions for user privacy. However our proposed method is successful enough to remove the issues which are associated with the previous methods. It is evident from above discussion that we have used successful rate and process time to estimate our proposed method, and compared its performances with EPCS (Efficient Pseudonym Changing Schemes for Location Privacy Protection) [13], RPCLP (Reputation-based Pseudonym Change for Location Privacy in Vehicular Networks) [83] and MODP (Mix-zones Optimal Deployment for protecting

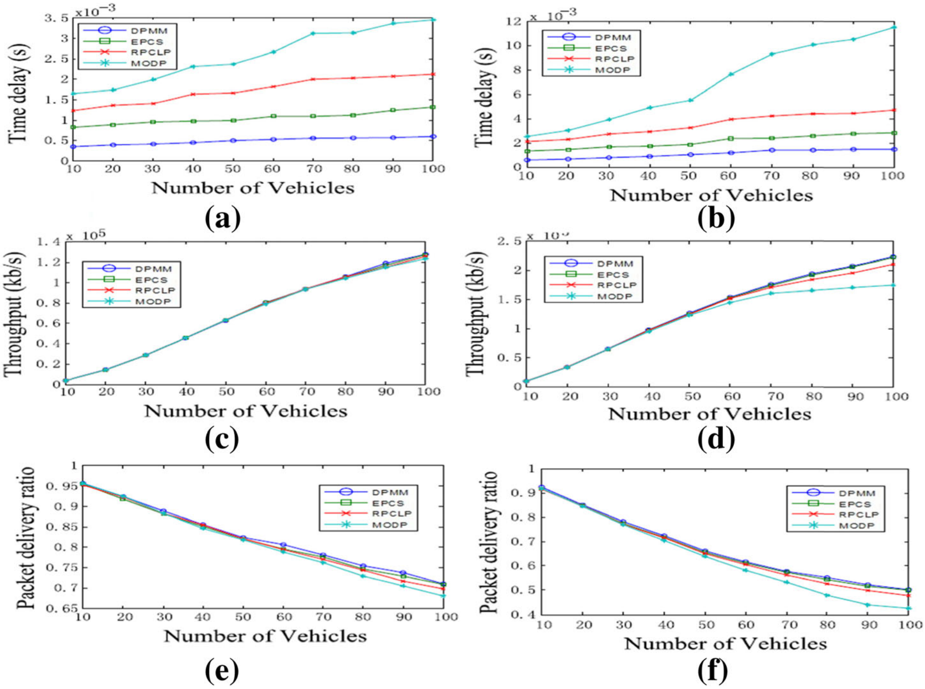


Fig. 9 Performace Evaluation

location Privacy) [76]. Calculation of the processing time inside the mix zone will not contain a time to send a request in EPCS (Efficient Pseudonym Changing Schemes for Location Privacy Protection) [13]. We compared successful rates of our method with three existing schemes varying with different mix-zones as shown in Fig.13. The total number of vehicles in the network are 10,000. DPMM has shown a successful rate at a value of 1. However, when compared with EPCS, MODP and RPCL, they have shown a lower successful rate. Moreover,

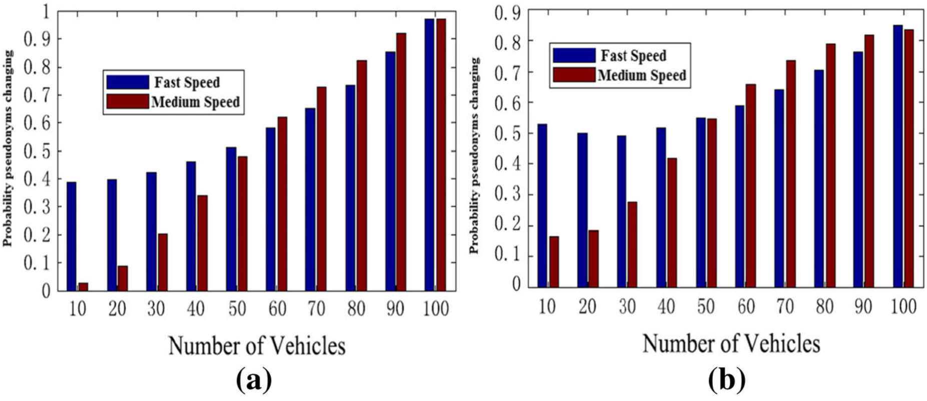


Fig. 10 Probability pseudonyms changing in various speed

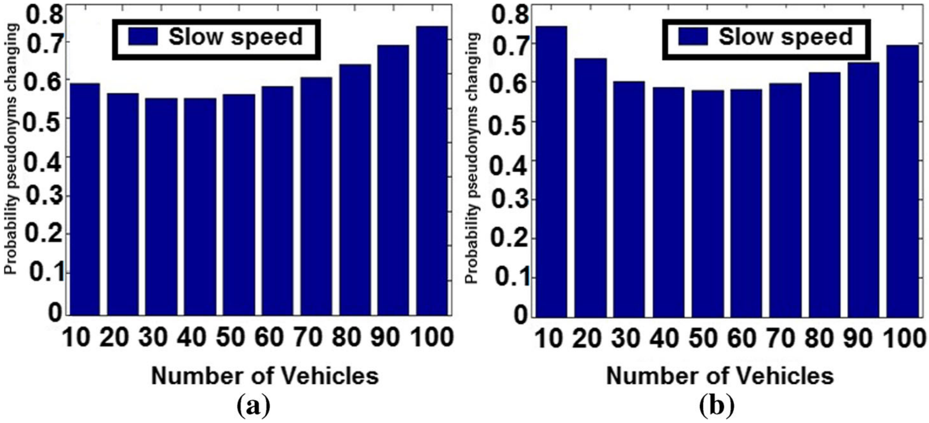


Fig. 11 Probability pseudonyms changing in various speed

the results verified that vehicle change their dynamic pseudonyms on the basis of the number of neighboring vehicles, as depicted in Fig. 14.

However, DPMM scheme goes up quickly when total number of vehicles increases, and process time is up to 380 s when the total number of vehicles becomes 600 as shown in Fig.15 where we compared processing times of three existing schemes.

5 Conclusion

In this research, we proposed an advanced method to improve user privacy in terms of dynamic pseudonyms, while focusing on multiple mix-zones over road networks. Our technique is based on multiple mix-zones using advanced cryptographic communication schemes to protect user privacy against various attacks, where number of pseudonym search user requests are limited in given timeframe. After having a detailed analysis of available literature,

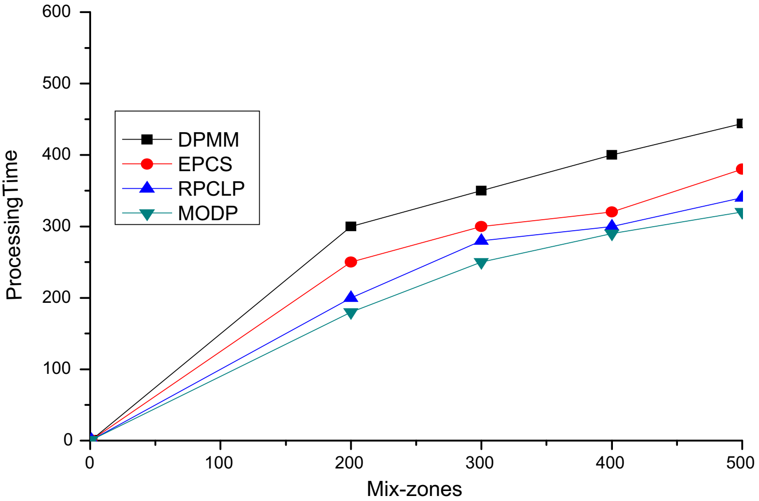
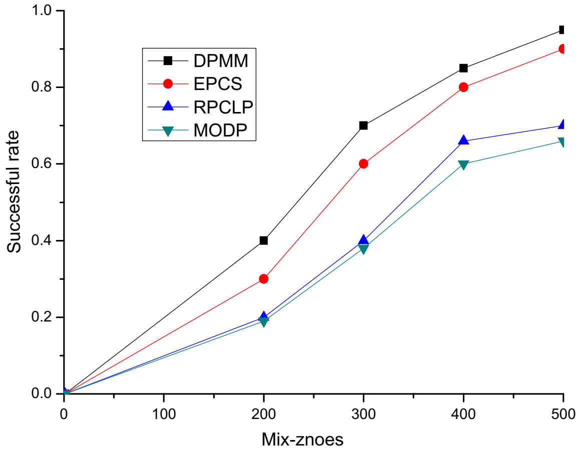


Fig. 12 Processing time vs Mix-zones

Fig. 13 Successful rate vs Mix-zones



we observed that existing schemes only deal with the methods that comprise of a single pseudonym change. However, an attacker can easily trace a single pseudonym change during any basic communication under mix-zone schemes. In this paper, we gradually encouraged each vehicle to change their pseudonym dynamically by using (DPMM) approach inside and outside mix-zone. We proposed a new reputation based dynamic pseudonym change protocol for location privacy protection. Moreover, we proposed a dynamic pseudonym based upon multiple mix-zones (DPMM) generation along with privacy protection, providing various parameters for defending against malicious attacks. We performed our simulation by using SUMO simulator and analyzed results by comparing with several existing pseudonym changing techniques. On the basis of detailed analysis of results, it has been inferred that our simulation results outperformed existing techniques such as EPCS (Efficient Pseudonym Changing Schemes for Location Privacy Protection) [13], RPCLP (Reputation-based

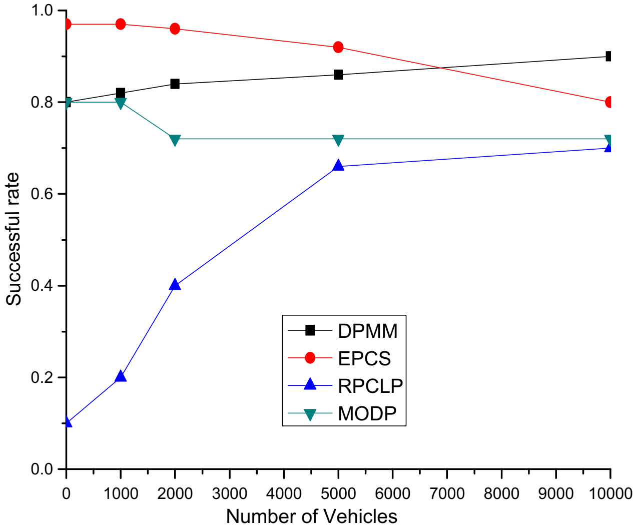


Fig. 14 Successful rate vs Number of vehicles

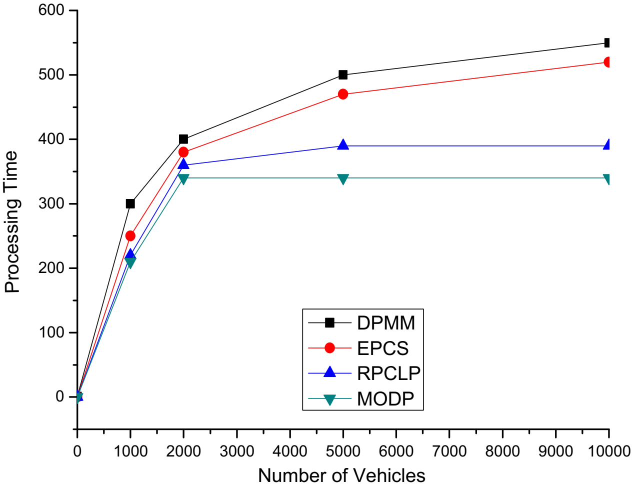


Fig. 15 Processing time vs Number of vehicles

Pseudonym Change for Location Privacy in Vehicular Networks) [83] and MODP (Mix-zones optimal deployment for protecting location privacy) [76]. Furthermore, we obtained better results in terms of achieving high privacy protection rate with a smaller number of pseudonym changes. In our future work, we will examine vehicle to vehicle communication privacy along with focusing on user behavior inside and outside mix-zones over road networks.

Acknowledgement We thank reviewers for their valuable comments/suggestions on the early version of the paper. Imran Memon & Qasim Ali contributed equally to this work.

Compliance with ethical standards

Competing interests The author(s) declare that there is no conflict of interest regarding the publication of this manuscript.

References

1. Aad I, Hubaux JP, Knightly EW (2008) Impact of denial of service attacks on ad hoc networks. IEEE/ACM Trans Networking 16:791–802
2. Adigun A, Bensaber BA, Biskri I (2013) Protocol of change pseudonyms for VANETs. 9th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks, Local Computer Networks Workshops (LCN Workshops), IEEE 38th Conference on. pp. 162–7, Sydney, NSW. ISBN: 978-1-4799-0539-3
3. Ahmad J, Sajjad M, Jan Z, Mehmood I, Rho S, Baik SW (2016) Analysis of interaction trace maps for active authentication on smart devices. Multimed Tool Appl:1–19. doi:10.1007/s11042-016-3450-y
4. Akhtar R, Leng S, Memon I, Ali M, Zhang L (2014) Architecture of hybrid mobile social networks for efficient content delivery. Wirel Pers Commun. doi:10.1007/s11277-014-1996-4
5. Akhtar R, Leng S, Memon I, Ali M, Zhang L (2015) Architecture of hybrid mobile social networks for efficient content delivery. Wirel Pers Commun 80(1):85–96

6. Bamba B, Liu L, Pesti P, Wang T (2008) Supporting anonymous location queries in mobile environments with privacygrid. WWW Proceedings of the 17th international conference on World Wide Web 237–246. doi:10.1145/1367497.1367531
7. Bartolini I, Moscato V, Pensa RG, Penta A, Picariello A, Sansone C, Sapino ML (2016) Recommending multimedia visiting paths in cultural heritage applications. Multimed Tool Appl 75(7):3813–3842
8. Beresford A, Stajano F (2003) Location privacy in pervasive computing. IEEE Pervasive Computing 2(1): 46–55
9. Bibmeyer N, Petit J, Bayarou KM (2013) Copra: conditional pseudonym resolution algorithm in VANETs. Wireless On-demand Network Systems and Services (WONS), 2013 10th Annual Conference on p 9–16
10. Bobek S, Nalepa GJ, Ligęza A, Adrian WT, Kaczor K (2014) Mobile context-based framework for threat monitoring in urban environment with social threat monitor. Multimed Tool Appl 1–22. doi:10.1007/s11042-014-2060-9
11. Buttyán L, Holczer T, Weimerskirch A, Whyte W (2009) Slow: a practical pseudonym changing scheme for location privacy in vanets. IEEE Vehicular Networking Conference, p 1–8
12. Carianha AM, Barreto LP, Lima G (2011) Improving location privacy in mix-zones for VANETS. Performance Computing and Communications Conference (IPCCC), 2011 I.E. 30th International p 1–6
13. Chen Y-S, Lo T-T, Lee C-H, Pang A-C (2013)Efficient pseudonym changing schemes for location privacy protection in VANETs. 2013 International Conference on Connected Vehicles and Expo (ICCVE). doi:10.1109/ICCVE.2013.185
14. Chmiel W, Dańda J, Dziech A (2016) INSIGMA: an intelligent transportation system for urban mobility enhancement. Multimed Tool Appl 1–32. doi:10.1007/s11042-016-3367-5
15. Engoulou RG, Bellaïche M, Pierre S, Quintero A (2014) VANET security surveys. Comput Commun 44:1–13
16. Freudiger J, Raya M, Félegyházi M, Papadimitratos P, Hubaux J-P, (2007) Mixzones for location privacy in vehicular networks. ACM Win-ITS
17. Freudiger J, Manshaei H, et al (2009a) On non-cooperative location privacy: a game-theoretic analysis. In: Proceedings of the ACM conference on computer and communications security(CCS). ACM, Chicago, p 324–337. doi:10.1145/1653662.1653702
18. Freudiger J, Shokri R, Hubaux JP (2009b) On the optimal placement of mix zones. Privacy Enhancing Technologies Symposium (PETS), Seattle p 216–234
19. Freudiger J, Manshaei MH, Boudec J-YL, Hubaux J-P (2010) On the age of pseudonyms in mobile ad hoc networks. INFOCOM, 2010 Proceedings IEEE, p 1–9
20. Freudiger J, Manshaei MH et al (2013) Non-cooperative location privacy. IEEE Transactions on Dependable and Secure Computing 10(2):84–98
21. Furini M, Tamanini V (2015) Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions. Multime Tool Appl 74(21):9795–9825
22. Gedik B, Liu L (2005) Location privacy in mobile systems: a personalized anonymization model. ICDCS Proceedings of the 25th IEEE International Conference on Distributed Computing Systems 620–629. doi:10.1109/ICDCS.2005.48
23. Ghinita G, Kalnis P, Skiadopoulos S (2007) PRIVE: anonymous location-based queries in distributed mobile systems. WWW Proceedings of the 16th international conference on World Wide Web 371–380. doi:10.1145/1242572.1242623
24. Gruteser M Grunwald D (2003) Anonymous usage of location-based services through spatial and temporal cloaking. MobiSys Proceedings of the 1st international conference on Mobile systems, applications and services 31–42. doi:10.1145/1066116.1189037
25. Guo S, Zeng D, Yang X (2014) Chameleon hashing for secure and privacy-preserving vehicular communications. IEEE Trans Parallel Distrib Syst 25(11):2794–2803. doi:10.1109/TPDS.2013.277
26. Gustav YH, Wang Y, Kamenyi DM, Zhang F, Memon I (2013) Velocity similarity anonymization for continuous query location based services. In 2013 International conference on computational problem-solving (ICCP) p 433–436. doi:10.1109/ICCPS.2013.6893578
27. Hamieh A, Ben-Othman J, Mokdad L (2009) Detection of radio interference attacks in VANET. In IEEE global telecommunications conference, GLOBECOM p 1–5
28. Härri J, Filali F, Bonnet C (2009) Mobility models for vehicular ad hoc networks: a survey and taxonomy. IEEE Communications Surveys & Tutorials 11(4):19–41
29. Huang L, Matsuura K, Yamane H, Sezaki K (2006) Silent cascade: enhancing location privacy without communication QoS degradation. In Proceedings of SPC p 165–180
30. Humbert M, Manshaei MH, et al (2009) On the optimal placement of mix zones: a game-theoretic approach. In proceeding of the 16th ACM conference on Computer and Communications Security p 324–337
31. Jiang D, Wanga X, Guo L (2009) An optimization method of large-scale IP traffic matrix estimation. AEU Int J Electron Commun 64(7):685–689

32. Jiang D et al (2011) Joint time–frequency sparse estimation of large-scale network traffic. Comput Netw 55(15):3533–3547
33. Jiang D, Xu Z, Zhang P Zhu T (2014) A transform domain-based anomaly detection approach to network-wide traffic. J Netw Comput Appl (40):292–306
34. Jiang D, Yao C, Xu Z et al (2015) Multi-scale anomaly detection for high-speed network traffic. Trans Emerg Telecommun Technol 26(3):308–317
35. Jiang D, Yuan Z, Zhang P, Miao L, Zhu T (2016a) A traffic anomaly detection approach in communication networks for applications of multimedia medical devices.A traffic anomaly detection approach in communication networks for applications of multimedia medical devices. Multimed Tool Appl 1–25. doi:10.1007/s11042-016-3402-6
36. D Jiang, L Shi, P Zhang, Ge X (2016b) QoS constraints-based energy-efficient model in cloud computing networks for multimedia clinical issues. Multimed Tool Appl 1–22. doi:10.1007/s11042-015-3239-4
37. Kamenyi DM, Wang Y, Zhang F, Memon I (2013) Authenticated privacy preserving for continuous query in location based services. J Comput Inf Syst 9(24):9857–9864
38. Li J (2016) A synthetic research on the multimedia data encryption based mobile computing security enhancement model and multi-channel mobile human computer interaction framework. Multimed Tool Appl:1–25. doi:10.1007/s11042-016-3662-1
39. Li Y, Chen D (2015) A learning-based comprehensive evaluation model for traffic data quality in intelligent transportation systems. Multimed Tool Appl 1–16. doi:10.1007/s11042-015-2676-4
40. Li M, Sampigethaya K, et al (2006) Swing & swap: user-centric approaches towards maximizing location privacy. WPES p 19–28
41. Liu X, Zhao H, Pan M, Yue H, Li X, Fang Y (2012) Traffic-aware multiple mix zone placement for protecting location privacy. Proc - IEEE INFOCOM p 972–980
42. Liu Y, He Z, Zhao S, Wang L (2016).An efficient anonymous authentication protocol using batch operations for VANETs. Multimed Tool Appl 1–21.doi:10.1007/s11042-016-3614-9
43. Lu R, Lin X, Luan TH, Liang X, Shen XS (2012) Pseudonym changing at social spots: an effective strategy for location privacy in vanets. IEEE Trans Veh Technol 61(1):86–96
44. Lu Y, Li L, Peng H, Yang Y (2015) An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography. Multimed Tool Appl 1–15. doi:10.1007/s11042-015-3166-4
45. Martinez FJ, Toh CK, Cano J-C, Calafate CT, Manzoni P (2011) A survey and comparative study of simulators for vehicular ad hoc networks. Wirel Commun Mob Comput 11:813–828
46. Mazurczyk W, Szaga P, Szczypiorski K (2014) Using transcoding for hidden communication in IP telephony. Multimed Tool Appl 70(3):2139–2216
47. Memon I (2015a) Authentication User's privacy: an integrating location privacy protection algorithm for secure moving objects in location based services. Wirel Pers Commun 82(3):1585–1600
48. Memon I (2015b) A secure and efficient communication scheme with authenticated key establishment protocol for road networks. Wirel Pers Commun 85(3):1167–1191
49. Memon I, Arain QA (2016) Dynamic path privacy protection framework for continuous query service over road networks. World Wide Web. 1–33. doi:10.1007/s11280-016-0403-3
50. Memon I, Mohammed MR, Akhtar R, Memon H, Memon MH, Shaikh RA (2014) Design and implementation to authentication over a GSM system using certificate-less public key cryptography (CL-PKC). Wirel Pers Commun 79(1):661–686
51. Memon I, Chen L, Majid A, Lv M, Hussain I, Chen G (2015a) Travel recommendation using geo-tagged photos in social Media for Tourist. Wirel Pers Commun 80(4):1347–1362
52. Memon I, Hussain I, Akhtar R, Chen G (2015b) Enhanced privacy and authentication: an efficient and secure anonymous communication for location based service using asymmetric cryptography scheme. Wirel Pers Commun 84(2):1487–1508
53. Memon MH, Li J-P, Memon I, Arain QA (2016) GEO matching regions: multiple regions of interests using content based image retrieval based on relative locations. Multimed Tool Appl 1–35. doi:10.1007/s11042-016-3834-z
54. Meyerowitz J, Choudhury R (2009) Hiding stars with fireworks:location privacy through camouflage in MOBICOM Proceedings of the 15th annual international conference on Mobile computing and networking 345–356. doi:10.1145/1614320.1614358
55. Milutinović M, Labus A, Stojiljković V, Bogdanović Z, Despotović-Zrakić M (2015) Designing a mobile language learning system based on lightweight learning objects. Multimed Tool Appl 74(3):903–935
56. Mishra T, Garg D, Gore MM (2011) A publish/subscribe communication infrastructure for VANET applications. In IEEE advanced information networking and applications (WAINA) workshops p 442–446
57. Moghraoui K (2015) An efficient pseudonym change protocol based on trusted neighbours for privacy and anonymity in VANETs p 93–99

58. Mokbel M, Chow C, Aref W (2006) The new casper: query processing for location services without compromising privacy. In VLDB Proceedings of the 32nd international conference on Very large data bases 763–774
59. Muraleedharan R, Osadciw LA (2009) Cognitive security protocol for sensor based VANET using swarm intelligence. In 43th IEEE Asilomar signals, systems and computers conference p 288–290
60. Ohta T, Ogasawara K, Kakuda Y (2010) End-to-end transfer rate adjustment mechanism for VANET. In 3rd Dependability conference, DEPEND p 1–6
61. Palanisamy B Liu L (2011) MobiMix: protecting location privacy with mix zones over road networks. Proc. of 27th IEEE International Conference on Data Engineering (ICDE'11) p 494–505
62. Palanisamy B, Ravichandran S, Liu L, Han B, Lee K, Pu C (2013) Road network mix-zones for anonymous location based services. In: Proceedings of the IEEE 29th international conference on data engineering (ICDE) p 1300–1303
63. Pan Y, Li J (2012) An analysis of anonymity for cooperative pseudonym change scheme in one-dimensional vanets. Computer Supported Cooperative Work in Design (CSCWD), 2012 I.E. 16th International Conference on p 251–257
64. Pan Y, Li J (2013a) Cooperative pseudonym change scheme based on the number of neighbors in VANETs. J Netw Comput Appl 36:1599–1609
65. Pan Y, Li J (2013b) Cooperative pseudonym change scheme based on the number of neighbors in VANETs. J Netw Comput Appl 36(6):1599–1609
66. Park KC, Shin H, Park WH, Lim JI (2015) New detection method and countermeasure of cyber attacks in mix networks. Multimed Tool Appl 74(16):6509–6518
67. Parno B, Perrig A (2005) Challenges in securing vehicular networks. In: Hot topics in networks (HotNets-IV) College Park, Maryland, November 2005
68. Sadhukhan P, Chatterjee N, Das A, Das PK (2010) A scalable location-based services infrastructure combining gps and bluetooth based positioning for providing services in ubiquitous environment. IMSAA 2010, p 15–17
69. Saini M, Atrey PK, Mehrotra S, Kankanhalli M (2014) W3-privacy: understanding what, when, and where inference channels in multi-camera surveillance video. Multimed Tool Appl 68(1):135–158
70. Sampigethaya K, Huang L, Li M, Poovendran R, Matsuura K, Sezaki K (2005) CARAVAN: Providing location privacy for VANET. In Proceedings of Embedded Security in Cars (ESCAR) 8
71. Shen J, Cai Y-J, Luo L (2015) A context-aware mobile web middleware for service of surveillance video with privacy. Multimed Tool Appl 74(18):8025–8051
72. Shiode N, Li C, Batty M, Longley P, Maguire D (2002) The impact and penetration of location-based services. CASA Working Paper 50. http://www.casa.ucl.ac.uk/working_papers/paper50.pdf. Accessed 23 Jun 2010
73. Sichitiu ML, Kini M (2008) Inter-vehicle communication system: a survey. IEEE Communications Surveys and Tutorials 10(2):88–105
74. Simulation of urban mobility (SUMO). Available at http://sumo.sourceforge.net
75. Soyoung P, Cliff ZC (2008) Reliable traffic information propagation in vehicular ad hoc networks. IEEE Sarnoff Symposium Conference p 1–6
76. Sun Y, Zhang B, Zhao B, Su X, Su J (2015) Mix-zones optimal deployment for protecting location privacy in VANET. Peer-to-Peer Networking and Applications 8(6):1108–1121015.
77. Tapascologne Project [Online]. Available: http://sourceforge.net/apps/mediawiki/sumo/index.php?title=TAPASCologne
78. U.S. Census Bureau.TIGER, TIGER/Line and TIGER-related products. Available at http://www.census.gov/geo/www/tiger/
79. U.S. Geological Survey http://www.usgs.gov
80. Virrantaus K, Markkula J, Garmash A, Terziyan V, Veijalainen J, Katanosov A et al (2001) Developing GIS-supported location-based services. In Proc. of the international conference on Web information systems engineering 2:66–75
81. Wang T, Liu L (2009) Privacy-aware mobile services over road networks in VLDB Endowment Hompage archive 2(1):1042–1053. doi:10.14778/1687627.1687745
82. Wu B, Chen J, Wu J, Cardei M (2007) A survey on attacks and countermeasures in mobile ad hoc networks. Springer Journal of Wireless Network Security 2:103–135
83. Ying B, Makraki D (2015) Reputation-based pseudonym change for location privacy in vehicular networks. IEEE ICC 2015- International Conference on Communications (ICC) 7041–7046. doi:10.1109/ICC.2015.7249449
84. Ying B, Makrakis D, Mouftah HT (2013) Dynamic Mix-Zone for Location Privacy in Vehicular Networks. IEEE Commun Lett 17(8)

Imran Memon B.S. Electronics 2008 from IICT University of Sindh Jamshoro, Sindh Pakistan. M.E. Computer Engineering from University of Electronic Science and Technology, Chengdu Sichuan China. He is towards Ph.D. from College of Computer Science and Technology, Zhejiang University. He got Academic Achievement Award 2011–2012 from UESTC China and also got Excellent Performance Award 2011–2012 from UESTC China. He published over 30 research papers in recent years. He serves as an organizing committee chairand TPC member more than 120 international conferences, as well as a reviewer for over 50 international research journals, including IEEE Transactions on Circuits and Systems for Video Technology ,IEEE Transactions on Image Processing, IEEE Transactions on Signal Processing, IEEE Transactions on Multimedia, ,IEEE Multimedia, IEEE Transactions on Industrial Electronics ,IEEE Signal Processing Letters, Journal of Electronic Imaging Information Sciences Computer Vision and Image Understanding, Image and Vision Computing, EURASIP Journal on Advances in Signal Processing ,Computer Standards & Interfaces, Circuits Systems and Signal Processing Journal of Information Science and Engineering, International Journal of Computers and Applications Far East Journal of Experimental and Theoretical Artificial Intelligence, IEE Proc. Vision, Image & Signal Processing, EURASIP Signal Processing IEE Proc. Information Security, Journal of Circuit, System, and Signal Processing, International Journal of Computers andApplications, LNCS Transactions on Data Hiding and Multimedia Security, Signal Processing International Journal of Pattern Recognition and Artificial Intelligence, IEEE Transactions on Information Forensics & Security, IEEE Transactions on Vehicular Technology, Transactions on Internet and Information Systems , Wireless personal communication, Computers & Electrical Engineering, Computer Networks, Wireless networks, Telecommunication systems and others. Current research interests; Artificial intelligence system, Network security, embedded system, Information security, Peer to Peer networks, Location based services, Road network,

Qasim Ali . is a Ph.D. candidate at School of Electronic Engineering, Beijing University of Posts and Telecommunication, China. He is currently working as an Assistant Professor in Department of Software Engineering Mehran University of Engineering and Technology, Jamshoro, Pakistan. He has completed his Bachelors in Software Engineering from Mehran UET Jamshoro in 2005 and completed his Masters in Information Technology in 2010. He is a Cisco Certified Academy Instructor (CCAI), Cisco Security Specialist Microsoft Certified System Engineer (MCSE), Sun Certified Java Programmer SCJP. His current research interest includes Location based services, Network Security and Indoor positioning.

Ms. Asma Zubedi , is a Ph.D. candidate at school of Economics and Management, Beijing University of Posts and Telecommunication, China. Her current research interest include Cyber security, ICT, service quality management and Big Data.

Farman Ali Mangi is pursuing PhD in the field of Radio Physics, University of Electronics Science & Technology, Chengdu, Sichuan, China. From February 1999 to 2008, he joined as Research Associate in Shah Abdul Latif University Khairpur, Sindh Pakistan. From August 2008 to 2013, he was appointed as Lecturer in the department of Physics & Electronics at SALU, Khairpur, Sindh, Pakistan. Currently, he is working as Assistant Professor in the department of Physics & Electronics, Shah Abdul Latif University, Khairpur, Sindh, Pakistan. He has presented his research work in different countries such as China, Thailand and Pakistan. He received China Scholarship Council (CSC) excellent international student research award for the academic year 2015/2016. His research interests included Electronics, Antenna and Propagation, LASER Atomic Spectroscopy and Material Physics. He has authored/co-authored more than 45 technical journals and conference papers.